

TAB

CONTENTS

TAB

COMPARISON	Analysis of Differences Between the New and Old Executive Orders
CLASSIFICATION	Principles, Authorities, Procedures, Markings, Record Holdings, General Statistics
DECLASSIFICATION	CIA Regulations, History of Procedures, Copy of Mr. Colby's Comments to Mr. Ehrlichman, Memo for DCI on "Foreign Relations" Series
CLEARANCES	Personnel Security: Authorities, Statistics, Background Investigation Polygraph Program Processing Reinvestigation Program Investigation Cost Factors Security Review Procedures DCI Memo to Mr. Ehrlichman on Reduction of Clearances
DCI on DISCLOSURES	Memoranda
NEW E. O.	A copy of the New Executive Order 11652

ANALYSIS OF DIFFERENCES BETWEEN
THE NEW AND OLD EXECUTIVE ORDERS

INTRODUCTION

The new Executive Order mentions conduct of foreign relations in addition to national defense. (Throughout the new Order national defense and conduct of foreign relations are termed national security). The old Order mentioned national defense only.

1. Security Classification Categories

In the new Order classified information is defined in terms of whether the information, if disclosed to unauthorized persons, could reasonably be expected to cause damage to the national security. Executive Order 10501 is defined in terms of whether the information, if disclosed to unauthorized persons could result in damage or could be prejudicial. The words could result in the old Order permitted classification of a document to cover extremely remote possibilities of damage or prejudice while the new Order requires reasonableness before a classification category can be utilized. The term "national security" as used in the new Executive Order includes both national defense and foreign relations matters. The use of the term "national security" rather than "national defense" recognizes that the category of information requiring protection is broader than military information alone, and is also more consistent with the provisions of the Freedom of Information Act which exempts from possible disclosure matters that are "specifically required by Executive Order to be kept secret in the interest of the national defense or foreign policy."

The three categories of classified information--Top Secret, Secret and Confidential--prescribed in Executive Order 10501 are written in the new Order. The distinctions between the three

categories still turn on the degrees of damage to the national security that could result from failure to protect the information from disclosure. The old Order cited compromise of "intelligence operations" as an example of damage. The new Order amended this to "sensitive intelligence operations."

2. Authority to Classify

Under Executive Order 10501, 38 Departments and Agencies had the authority to classify at the Top Secret level which is inclusive of authority to classify at the Secret and Confidential level. Under the new Executive Order, only 12 Departments and Agencies plus such offices in the Executive Office of the President as the President may designate in writing are so authorized. An additional 13 Agencies are delegated the authority under the new Executive Order to classify information at the Secret level.

The new Executive Order provides authority to delegate within a Department or Agency only to a limited number of officials. Top Secret original classification authority may not be delegated below the level of the principle deputies or assistants of major elements of the Department or Agency. In the 13 Agencies authorized to originally classify information Secret, classification authority may not be delegated below senior principle deputies or assistants. Under Executive Order 10501 original classification authority at the Top Secret level can be delegated to any person employed by the Department or Agency.

3. Authority to Downgrade and Declassify

Executive Order 10501 requires the heads of the Departments or Agencies originating classified information or material to designate persons to be responsible for continuing review of such classified information or material on a document-by-document category, project, program or other systematic basis for the purpose of declassifying or downgrading. Usually only individuals who had original classification authority were permitted to declassify.

The new Order, by specifically authorizing the Heads of the Departments or Agencies to delegate to individuals who do not have original classification authority the authority to declassify or downgrade, has increased the potential of the Departments or Agencies for increasing their capability to downgrade or declassify.

4. Classification

The Executive Order just issued establishes a new guiding principle--each person possessing original classification authority shall be held accountable for the propriety of his classification actions and can be reprimanded for overclassification and unnecessary classification.

To enable enforcement of this principle, the new Executive Order provides that information and material classified under the Order shall indicate on its face the identity of the highest authority authorizing the classification, unless the Agency involved shall have provided some other method of identifying him. If the signer or authenticator of a document also authorized its original classification, no further annotation as to his identity is required.

5. Declassification and Downgrading

Under Executive Order 10501, all information classified at the Top Secret, Secret or Confidential level is also required to be grouped into one of four categories for purposes of downgrading and declassification.

Group 1 information and material is excluded from automatic downgrading and declassification. It consists of information or material originating with foreign governments or international organizations, information and materials protected by statute, such as that falling within the purview of the Atomic Energy Act, and information or materials requiring special handling, such as intelligence or cryptology.

Group 2 information or material is also exempt from automatic downgrading and declassification. It consists of extremely sensitive information or material which the Head of the Agency or his designee designates.

Group 3 information or material is exempt from automatic declassification, but is subject to automatic downgrading at 12-year intervals until it reaches the lowest classification. It consists of that information or material which warrants some degree of classification for an indefinite period.

Group 4 includes all classified information or material not falling in Groups 1, 2 or 3 and is subject to downgrading at 3-year intervals and automatic declassification 12 years after the date of original issuance.

Under the new Executive Order, separate groupings for purposes of downgrading and declassification are dispensed with. In lieu of the grouping system, a General Declassification Schedule is prescribed, to which limited exceptions are specified and subjected to special rules for downgrading and declassification.

The general downgrading and declassification schedule is as follows: Top Secret information is automatically downgraded to Secret at the end of 2 years from the date of original classification; further downgraded to Confidential at the end of 4 years from date of original classification; and is declassified at the end of 10 years from the date it was originated.

Secret information is automatically downgraded to Confidential at the end of 2 years and automatically declassified at the end of 8 years from the date it was originated.

Confidential information is automatically declassified at the end of 6 years from the date it was originated.

This provides for an automatic downgrading and declassification schedule at intervals of 2 years, 4 years and 10 years as compared to the most rapid downgrading and declassification under the old system--that applicable to Group 4--at intervals of 3 years, 6 years and 12 years from original date of classification.

Four limited and specific categories of information are authorized to be exempted from the General Declassification Schedule specified in the new Executive Order. The specific exemption category must be specified in writing on the document or material. The four exemptions cover information or material which fall into one of the four following categories:

A. Classified information or material furnished by foreign governments or international organizations and held by the United States on the understanding that it be kept in confidence.

B. Classified information or material specifically covered by statute, or pertaining to cryptography, or disclosing intelligence sources or methods.

C. Classified information or material disclosing a project, plan, installation or system or a specific foreign relations matter the continuing protection of which is essential to the national security.

D. Classified information or material the disclosure of which would place a person in immediate jeopardy.

Information or material falling into one of the categories eligible for exemption may thus escape automatic downgrading and declassification. However, such material is made subject to a mandatory classification review any time after the expiration of 10 years from date of origin upon request by a Department or a member of the public.

In addition to the mandatory review upon request at the end of 10 years, the new Executive Order provides for automatic declassification at the end of 30 years from origination of all classified information unless the Head of the originating Department personally determines in writing at the end of 30 years that continuing protection is essential to the national security or that its disclosure would place a person in immediate jeopardy. Under the provisions of Executive Order 10501, classified information falling in Groups 1, 2 and 3 was subject to no automatic declassification.

The Executive Order provides that information classified before the effective date of the new Order, regardless of the Group to which it was assigned, shall be subject to mandatory review at the end of 10 years from origination in accordance with the rules which apply to the mandatory review for information or material

exempted from the General Declassification Schedule under the new Order. Similarly, all information and material classified before the effective date of the new Order which is 30 years or more old shall be systematically reviewed for declassification by the Archivist of the United States.

6. Access, Markings, Safekeeping, Accountability, Transmission, Disposition and Destruction of Classified Information and Material

The old Order gave specific instructions concerning Markings of Classified Material (Section 5); Custody and Safekeeping (Section 6); Accountability and Dissemination (Section 7); Transmission (Section 8) and Disposal and Destruction (Section 9).

The new Order in Section 6 states that "The President acting through the National Security Council shall issue directives which shall be binding on all Departments or Agencies to protect classified information from loss of compromise." It also lists seven policy statements and states that such directives shall conform to these policies.

7. Implementation and Review Responsibilities

The old Order charged the National Security Council to conduct continuing review to ensure compliance thereto, to ensure that classified information is protected. The new Executive Order provides that each Department or Agency originating or handling classified information shall form a Departmental or Agency committee to act on all suggestions and complaints with respect to the Department's or Agency's administration of the Order. The committee is to be chaired by a senior member of the staff of the Head of the Department or Agency.

Even more important, however, the Order establishes an Interagency Classification Review Committee under the National Security Council. This Committee is to be composed of representatives of the Departments of State, Defense and Justice, the Atomic Energy Commission, the Central Intelligence Agency, and the National Security Council staff. The Chairman is to be designated by the President.

The Interagency Classification Review Committee has the following responsibilities:

- A. To monitor Department actions to ensure compliance with the provisions of the Executive Order and such implementing directives as are promulgated by the National Security Council;
- B. To receive, consider and take action on suggestions and complaints from persons within or outside the Government on the administration of the Executive Order; and
- C. In consultation with the affected Department or Departments, to assure that appropriate action is taken on suggestions and complaints.

The Executive Order requires Departments and Agencies to furnish the Committee any particular information or material needed by the Committee to carry out its functions. In addition, prior to 1 June 1972 each Agency or Department will submit to the Committee for approval a copy of the regulations it proposes to adopt pursuant to the new Order.

8. Material Covered by the Atomic Energy Act

There is no difference between Executive Order 10501 and the new Order.

9. Special Departmental Arrangements

The originating Department or other appropriate authority may impose, in conformity with the provisions of this Order, special requirements with respect to access, distribution and protection of classified information and material, including those which presently relate to communications intelligence, intelligence sources and methods and cryptography. No such authority was granted in Executive Order 10501.

10. Exceptional Cases

The new Order does not significantly amend Executive Order 10501 in this field. A person or Department not having original classification authority but originating information which is believed to require classification, shall protect the information as if it were

classified and shall request an appropriate Department or Agency to make the classification decision.

11. Declassification of Presidential Papers

The Archivist of the United States shall have the authority to review information and material classified by a President, his White House Staff or special committee or commission appointed by him and which the Archivist has in his custody at any archival depository, including a presidential library. This provision was not in Executive Order 10501.

12. Historical Research and Access by Former Government Officials

There is no change in the new Order from the Historical Research provisions of Executive Order 10501; however, the new Order will permit the Head of an Agency to grant access to a person previously occupied in a policy making position to which he had been appointed by the President if such access is clearly consistent with the interest of national security and the Head of the Agency takes appropriate steps to assure that the classified information or material is not published or otherwise compromised. Access granted a person by reason of having previously occupied a policy making position shall be limited to those papers which the former official originated, reviewed, signed, or received while in public office.

13. Administrative and Judicial Action

This section permits administrative reprimands to individuals who repeatedly abuse the classification process; i.e., unnecessary classification or overclassification. In addition, the Head of a Department or Agency is directed to take prompt and stringent administrative action against any employee who is responsible for unauthorized disclosure of classified material. Executive Order 10501 did not contain a provision for reprimanding individuals abusing the classification process.

General Analysis of the New Executive Order as it Affects CIA

By specifically exempting classified information and material pertaining to intelligence sources and methods from the General Declassification Schedule the new Order assures that such sources and methods can be protected for as long a time as protection is needed. I do not anticipate any substantive problems in carrying out intent of the new Executive Order.

CLASSIFICATION

STATINTL [REDACTED]

1. Principles for Classification

- a. Classification of information and material is considered in terms of the potential effects its unauthorized disclosure has on the defense intelligence efforts of the nation.
 - b. Classification of information and material is in accordance with the definition of the security classification categories.
 - c. Classification is based upon degree of secrecy warranted for control of the information and not upon the desirability of restricting access under the need-to-know principle.
 - d. Classification of information and material is based on content and not necessarily on relationship to other documents.
 - e. Reference to classified information or material when the reference does not in itself reveal the substance of classified defense or intelligence information shall not be classified.
 - f. A document or material shall bear a classification at least as high as that of its highest classified components. It will bear only one overall classification notwithstanding paragraphs and sections which bear different classifications or no classification.
2. All CIA documents and material are excluded from automatic downgrading.
3. Authority to Classify

The CIA Classification Control Officer, Assistant Classification Control Officers and Authorized Classifiers are the only persons authorized to apply an original classification to information or material.

4. Classification Network

- a. Network was established to control the classification of information or material against unauthorized disclosure.
- b. Network under jurisdiction of Assistant Director for Central Reference consisting of:
 - (1) The CIA Classification Control Officer
 - (2) Assistant Classification Control Officers
 - (3) Authorized Classifiers
- c. Deputy Directors and Operating Officials designate as many Assistant Classification Control Officers within their areas of jurisdiction as necessary for effective administration and supervision of classification procedures and activities.
- d. Assistant Classification Control Officers may designate as many Authorized Classifiers as required.
- e. Notification is given in writing to the CIA Classification Control Officer of all individuals so designated.

5. When security classification categories do not apply, the following internal Agency control markings may be considered [REDACTED]

STATINTL

- a. Administrative-Internal Use Only. This control marking may be used for unclassified, non-sensitive administrative information which should not be disseminated outside of CIA.
- b. For Official Use Only. This control may be used whenever intelligence or intelligence information does not warrant a defense (national security) classification, but does require some dissemination limitation. Intelligence or information bearing this marking may be used for official purposes by

foreign governments which have been authorized to receive it by the originating agency. It may be disclosed to non-Government persons and organizations only with permission of the originating agency. This control marking is used alone and never in conjunction with a defense (security) classification. Some reasons for requiring such dissemination control are: protection under copyright, libel, slander, and communication laws; and protection for moral, ethical, or legal reasons.

6. There are other control markings [REDACTED] which are used with security classification categories, such as:

STATINTL

a. WARNING NOTICE--SENSITIVE SOURCES AND METHODS INVOLVED

This marking shall be employed in the absence of any other suitable marking to inform all recipients that the information is sensitive and requires special controls and a severely limited distribution. For the purpose of this marking, such intelligence is identified as that classified intelligence, the unauthorized disclosure of which could lead to counteraction

(1) jeopardizing the continued productivity of intelligence sources or methods that provide intelligence vital to the national security, or

(2) offsetting the value of intelligence vital to the national security.

b. CONTROLLED DISSEM

This marking is used where source protection, including proprietary interests of commercial sources would warrant limiting the dissemination of the document. This marking

may also be applied for dissemination control purposes to assist in identifying that intelligence material which by category or classification is by USIB-approved policy and other directives prohibited from dissemination to contractors.

c. NO DISSEMINATION ABROAD

Employed to preclude the dissemination of a document outside the States of the United States except as determined by the originator to satisfy special conditions.

d. BACKGROUND USE ONLY

Employed to preclude the inclusion of the information in any other document or publication. Intended solely to control the use of the information.

e. NO FOREIGN DISSEM

Employed when the originator predetermines that intelligence information must not be released in any form to foreign governments.

f. CIA INTERNAL USE ONLY

Used for classified information which if disclosed would violate existing Agency policy regarding protection of sources and methods. Classified intelligence or classified information so marked may not be released or shown to anyone outside the Agency without permission of the originating office. Within the Agency, classified intelligence or classified information so marked may be released only to full time Agency employees and is not disseminated to consultants, external projects, or reserve personnel on short-term active duty unless permission of the originating office is obtained.

STATISTICS (Estimates)

1. 3,500 - persons authorized to classify documents at all levels
2. 760 - persons authorized to classify documents Top Secret under new order
3. 2% - CIA documents classified Confidential
88% - Classified Secret
10% - Classified Top Secret
4. 675,000 - Number of CIA classified intelligence documents and cables produced annually (does not include classified admin reports, memoranda, and notices, for which no estimate is available)
5. 1,070,000 - Documents received annually from other Government agencies
6. 349,400 - Cubic feet - Total volume of records on hand in offices and storage (FY 1971)
7. 72,940 - Cubic feet - Volume of records destroyed (FY 1971)
8. Special files in cubic feet
 - 1,326 - Lebanon Conflict
 - 4,982 - Cuban Missile Crisis
 - 5,672 - Bay of Pigs

RECORD HOLDINGS

1957 - 1971

Fiscal Year	Totals (Cubic Feet)
1957	153,700
1958	184,800
1959	223,600
1960	215,200
1961	225,600
1962	241,800
1963	244,000
1964	275,800
1965	288,300
1966	286,200
1967	330,400
1968	355,900
1969	332,400
1970	330,800
1971	349,400

Top Secret 10%

Secret 88%

Confidential and Unclassified 2%

CONFIDENTIAL
CONTINUATION

DECLASSIFICATION

1. The Central Intelligence Agency regulations provide for an orderly procedure for declassification and reclassification of documents. The regulations set forth that:

"Classified information or material shall be reviewed on a continuing basis for the purpose of determining the current appropriateness of the classification assigned with a view to declassification or reclassification where appropriate."

2. In the years immediately following the issuance of Executive Order 10501, the Agency had a formal program of classification review to upgrade or declassify all RESTRICTED material. EO 10501 had eliminated that classification. We established a Classification Control Network which regularly issued reclassification bulletins. Now our Central Top Secret Control activity continues to issue semiannual notices of Top Secret documents which have been downgraded. Because of cost constraints, manpower reductions and the increased volume of classified documents we have collected our efforts are limited to responding to ad hoc internal and external requests for downgrading of specific CIA documents. Individual requests are handled on an expeditious basis. About 100 CIA TS documents were downgraded in 1971. A review project is underway within the Agency to declassify the [REDACTED] publication "Trends and Communist Propaganda" and earlier titles in this series from 1947 to 1966. We continue to review OSS material and have declassified some of it in response to official and public requests.

STATSPEC

3. We are in the process of amending our regulations to insure that the provision of the new Executive Order are implemented within the Agency. I believe the new Executive Order is a realistic approach to the problem of classification, reclassification and downgrading and the CIA will, of course, adhere to its provisions. Although specific areas of concern may develop as we work with the document, I am confident that these matters can be resolved within the mechanism of the Interagency Classification Review Committee established under Section 7 of the new Order.

7 December 1971

MEMORANDUM FOR: The Honorable John D. Ehrlichman
Assistant to the President
(Domestic Affairs)

SUBJECT : Declassification

1. Bill Colby told me of his lunch with you and your discussion of declassification. We have produced the attached outline summary of the problem and a possible solution for your consideration. It obviously would require further detail if it were to be adopted. The important thing, however, is the degree to which it fits your general thinking.

2. If there is anything else we can do to help on this problem, please let me know.

/s/

Richard Helms
Director

Attachment as stated

~~CONFIDENTIAL~~

C
O
P
Y

~~CONFIDENTIAL~~

SUBJECT: Declassification

1. From the parochial perspective of an intelligence officer, the major problem inherent in declassification relates to the risk of compromising operational sources and methods. A report several years old whose substantive content is no longer politically delicate, for example, could nonetheless compromise a still producing source who, indeed, might now be even better or more strategically placed than he was when he provided the report in question. What an intelligence service needs (and strives) to protect are the techniques it employs in going about its business and the human assets, especially foreign nationals, it uses or has used in the past. From an intelligence officer's standpoint, therefore, a document's sensitivity is a direct function of the extent to which that document could compromise sources or methods if it were to fall into unauthorized hands or pass into the public domain.

2. When we address the issue of declassifying the intelligence contribution to major policy decisions or historical events, we are talking about at least three separate types of documents.

(a) Finished Intelligence. This appears in the form of National Intelligence Estimates or special memoranda, drawn from all sources, recounting the facts and assessing a situation. In most cases, declassification of such documents would not jeopardize sources and methods, since the sources of the facts and assessments are usually not stated or are obscured so that they are not apt to be disclosed by declassification of the document. The documents may occasionally refer to the original source of material contained therein, but such references could be edited out or generalized so that the original source remains protected. This would require of course careful review of any such material prior to declassification with this thought in mind.

(b) Disseminated Intelligence. Some disseminated intelligence, such as technical or communications intelligence, reflects its origins in very specific terms so that declassification would almost inevitably result in the disclosure of the

~~CONFIDENTIAL~~

C
O
P
Y

~~CONFIDENTIAL~~

source. In other cases, such as clandestinely acquired intelligence, generalized source descriptions are used in the disseminations, so that the exact identity of the source remains concealed. In all these categories, the passage of time may to some extent alleviate the damage caused by a disclosure of the source, e.g., the fact that we were reading Japanese codes during World War II is hardly a sensitive matter any more. On the other hand, with respect to some of these sources, the passage of time may not relieve the sensitivity of the matter, particularly on material provided to us by a friendly foreign intelligence service which expects us to keep their relationship with us a permanent secret. Thus in the category of disseminated intelligence, a considerably greater job of editing might be necessary to separate items which could be declassified from those which should not be.

(c) Intelligence Operational Traffic. There is a great deal of this material which in almost all cases should not and can not be declassified without a highly inappropriate disclosure of intelligence sources and methods. The material itself is frequently written with special code names which may be valuable in the future. Also the methodology revealed may show things about our service which could be of advantage to an unfriendly power. The true names of our agents and the precise techniques of our operations should in no event be disclosed even after many years.

3. Cutting across the specific problems of declassifying intelligence material is the way our government does business in these times. Thanks to the enormous improvements in communications technology, the government utilizes a flood of separate papers and documents in the course of doing its business. In order to make these manageable at the key decision levels, these raw documents must be collated, summarized and analyzed in the form of over-all reports. This of course is what happens to raw intelligence material through the National Intelligence Estimates and similar documents. Decision-making on major national events is almost always based on the refined product rather than the raw. As noted above, the refined product raises considerably fewer problems of declassification than the raw. For the few cases in which raw documents are used in decision-making, edited versions might be provided.

C
O
P
Y

~~CONFIDENTIAL~~

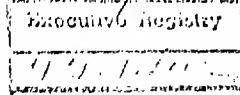
~~CONFIDENTIAL~~

4. Another factor to be considered is the inter-agency nature of most such major events today. Thus no single department or agency could give an over-all view of a major national event on the basis only of material available to it. The Pentagon Papers display this weakness.

5. A possible solution to the problem might lie in centralizing the production of official histories of selected major events. An historian might be added to the White House staff or the Archivist of the United States might be assigned this responsibility. This officer could serve as a point of coordination and tasking of the various departments and agencies to contribute to a national account of a major event. Department or agency contributions could thus be consolidated into a single over-all account. From the point of view of the intelligence community, this would permit summarization of material considered significant to the event to protect intelligence sources and methods, rather than declassifying raw material. It would also put the focus of the account on the key documents actually used at the national level rather than seeking the impractical aim of declassifying all raw material. Lastly, it would provide an over-all context in which individual raw documents would find a proper place, rather than causing sensational misunderstanding, if and when they came to public notice.

6. Such studies would not satisfy the history purists, of course, but they could meet the legitimate needs of the general public. Criticism could be made that an administration was writing its own histories. The proof of this pudding would be in the eating, i. e., whether the resulting studies were truly objective. The Pentagon Papers have not been subjected to this accusation nor are the Foreign Relations series produced by the Department of State or the studies produced by the Office of Military History.

C
O
P
Y



THE WHITE HOUSE
WASHINGTON

March 8, 1972

REC'D 7/15/72

MEMORANDUM FOR

THE DIRECTOR OF CENTRAL INTELLIGENCE

Subject: Acceleration of Publication of "Foreign
Relations" Series

I have today instructed the Secretary of State to institute a program to reduce the time lag of the official documentary series "Foreign Relations of the United States," published by the Department of State, from 26 to 20 years.

The Department of State, in carrying out this instruction, will be seeking the assistance of your department or agency in the collection and declassification of the material in question. I ask that you cooperate fully with the Secretary of State to meet the above objectives in the most expeditious manner and to the maximum extent consistent with the requirements of national security.

A handwritten signature in black ink, appearing to read "Richard Nixon".

FOR IMMEDIATE RELEASE

March 8, 1972

Office of the White House Press Secretary

THE WHITE HOUSE

March 8, 1972

MEMORANDUM FOR

THE SECRETARY OF STATE

Subject: Acceleration of Publication of "Foreign Relations" Series

The official documentary series "Foreign Relations of the United States," published by the Department of State, has for many years provided the American public with an indispensable perspective on our Nation's history. The materials now being published, however, relate to the events of 1946, and I think that in the interests of a better informed public the length of time between event and publication should be shortened. Accordingly, I ask that, without impairing the quality and comprehensive nature of the series, you immediately institute a program to reduce this time lag to 20 years. Your objective should be to make this reduction within the next 3 years and to keep the publication point at 20 years from then on.

In order to achieve this goal in the most expeditious manner, I am today instructing the Secretary of Defense, the Director of Central Intelligence, and the Assistant to the President for National Security Affairs to cooperate fully with you in collecting and declassifying the appropriate materials to the maximum extent consistent with the requirements of national security.

RICHARD NIXON

#

PERSONNEL SECURITY AUTHORITIES

The basic statutory authority on which the Personnel Security Practices and Procedures of the Central Intelligence Agency are based is the National Security Act of 1947 (as amended, 1949). Under Section 102d(3) of this Act, the Director is personally charged with protecting intelligence sources and methods from unauthorized disclosure. The Director has also declared all positions in the Central Intelligence Agency occupied by staff employees to be sensitive positions within the meaning of Section 3(b) of Executive Order 10450. Finally, there are numerous regulations of the Central Intelligence Agency concerning compliance with security regulations, the clearance of personnel for duty with the Agency, the security processing of personnel for entrance on duty, separation, leave and official absence, the control of personnel security files, the marriage of employees, the travel of close relatives to Communist controlled areas, limitations on outside employee activities, and assignments involving risk of capture.

25X9

Approved For Release 2001/04/01 : CIA-RDP83-01022R000100050022-5

Next 3 Page(s) In Document Exempt

Approved For Release 2001/04/01 : CIA-RDP83-01022R000100050022-5

POLYGRAPH PROGRAM

At present, the polygraph is utilized as an aid to the personnel security process in (a) the security investigation and clearance of applicants for employment; and (b) as a part of the security reinvestigation process of employees on duty to ensure their continued security reliability. The polygraph program is voluntary and all applicants and employees are requested to participate on a voluntary basis. The Office of Security is solely responsible for the conduct of the polygraph program of the Agency, including the training of polygraph examiners and the supervision and administration of the polygraph program.

No person will be polygraphed who has a history of serious cardiac trouble, a serious physiological deformity or who has a serious physical or personal problem at the time.

Polygraph reports are maintained exclusively within the Office of Security on a special controlled basis. Only those officers having a direct responsibility for personnel security evaluations may have access to reports of polygraph interviews concerning staff employees or applicants.

STATINTL

Approved For Release 2001/04/01 : CIA-RDP83-01022R000100050022-5

Next 5 Page(s) In Document Exempt

Approved For Release 2001/04/01 : CIA-RDP83-01022R000100050022-5

COST FACTORS

Set forth below are the results of a September 1970 analysis and comparison with Fiscal Year 1969 on costs of field investigations, various Agency clearances, and polygraph examinations.

A. Field Investigations	FY 1969	\$279.76
	FY 1970	285.52
B. Covert Approvals	FY 1969	\$ 63.24
	FY 1970	60.33
C. Overt Clearances	FY 1969	\$ 49.65
	FY 1970	45.11
D. Polygraph Examinations	FY 1969	\$160.23
	FY 1970	154.92
E. TOTAL COST OF A CASE (Includes Investigations, Average Covert/Overt Clearances & Polygraph)	FY 1969	<u>\$496.43</u>
	FY 1970	<u>\$493.15</u>

There has been no recent cost analysis but there have been pay increases and costs have generally risen. It is estimated that the total cost of a case at the present time is between \$500.00 and \$550.00.

SECURITY REVIEW PROCEDURES

With respect to CIA Staff Employees, the Director of Personnel has the responsibility of convening Personnel Evaluation Boards in order to review significant problem cases, and this is done on a regular basis. There are also occasions when more senior Executive Review Panels are convened at the Directorate level. If a case should justify such action, the Director of Central Intelligence has the authority to terminate a CIA Staff Employee under the provisions of the National Security Act of 1947, Section 102 (c) quoted below:

"Notwithstanding the provisions of section 652 (now 7501) of Title 5, or the provisions of any other law, the Director of Central Intelligence may, in his discretion, terminate the employment of any officer or employee of the Agency whenever he shall deem such termination necessary or advisable in the interests of the United States, but such termination shall not affect the right of such officer or employee to seek or accept employment in any other department or agency of the Government if declared eligible for such employment by the United States Civil Service Commission."

In Industrial Security cases, preliminary arrangements are made with the contractor to withdraw any clearance when it is deemed to be in the interests of national security. In normal circumstances, the Agency makes it a point not to utilize individuals unless they have been appropriately screened from a security standpoint. The cancellation or withdrawal of an industrial clearance is effected by:

- A. The completion or cancellation of the contract.
- B. The development of serious security information.
- C. The determination that an individual no longer has a "need to know."

~~CONFIDENTIAL~~

SECRET

17/3/71
17/3/71

RE:

MEMORANDUM FOR: Mr. John D. Ehrlichman
Assistant to the President for Domestic Affairs

SUBJECT : Security Clearance Review

1. This report responds to your request for a status report on steps which the Central Intelligence Agency has taken to effect reductions in clearances pursuant to the President's Directive of 30 June 1971.
2. The Agency's Security Clearance Review has resulted in the following clearance reductions:

TYPE AND NUMBER OF CLEARANCES CANCELED

	<u>Top Secret</u>	<u>Codeword</u>	<u>Total</u>
CIA Employees		490	490
Consultants	15	5	20
Employees of Contractors	966	1,791	2,757
<u>Grand Total</u>			<u>3,267</u>

3. Please let me know if any further clarification of the data is desired.

DIC/AM (jcc)

Richard Helms
Director

25X1A9a

D/S Rewritten O/ExDir [REDACTED] sfc